4)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-211191
(43)Date of publication of application : 11.08.1998

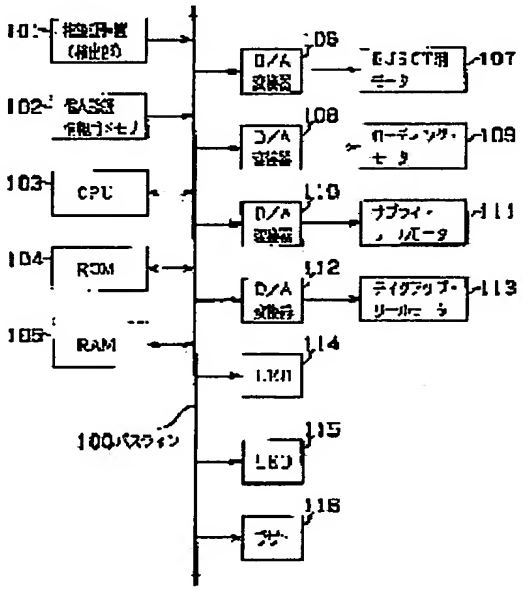
(51)Int.CI. A61B 5/117
G06T 7/00
H04L 9/32
H04N 5/76
// G06T 1/00

(21)Application number : 09-019208
(22)Date of filing : 31.01.1997

(71)Applicant : TOSHIBA CORP
TOSHIBA AVE CORP
(72)Inventor : YANAGIMOTO MASAO
YONEDA MINORU
OKUYAMA TAKEHIKO
YAMADADERA SHINJI
FUKUSHIMA MICHIHIRO
OSAWA SHINICHI

(54) RECORDING AND REPRODUCING DEVICE USING BIOLOGICAL INFORMATION AND ITS METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a recording and reproducing device using biological information and its method, which establishes absolute ownership with respect to the recording and reproducing device and a recording medium so as to protect copyright, privacy, etc.
SOLUTION: A finger authentication device 101 collates biological information detected by its detection part and that stored in a memory 102 for individual authentication information to execute the individual authentication operation of a person to be authenticated. At the time of passing individual authentication, a CPU 103 permits the operation of the recording and reproducing device to turn a motor 109 loading a cassette tape, a motor 107 ejecting a cassette and motors 111 and 113 driving a tape to be operable. On the other hand, at the time of not passing individual authentication, the CPU 103 does not permit the operation of the recording and reproducing device and stops the driving of all the motors.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－211191

(43)公開日　平成10年(1998)８月11日

(51)Int.Cl.[6]	識別記号	FI		
Ａ６１Ｂ	5/117	Ａ６１Ｂ	5/10	３２２
Ｇ０６Ｔ	7/00	Ｈ０４Ｎ	5/76	Ｚ
Ｈ０４Ｌ	9/32	Ｇ０６Ｆ	15/62	４６０
Ｈ０４Ｎ	5/76	Ｈ０４Ｌ	9/00	６７３Ｄ
// Ｇ０６Ｔ	1/00	Ｇ０６Ｆ	15/64	Ｇ

審査請求　未請求　請求項の数14　ＯＬ　（全 21 頁）

(21)出願番号　特願平9－19208

(22)出願日　平成９年(1997)１月31日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(71)出願人　000221029
東芝エー・ブイ・イー株式会社
東京都港区新橋３丁目３番９号

(72)発明者　柳本　正雄
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝マルチメディア技術研究所内

(72)発明者　米田　稔
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝マルチメディア技術研究所内

(74)代理人　弁理士　伊藤　進

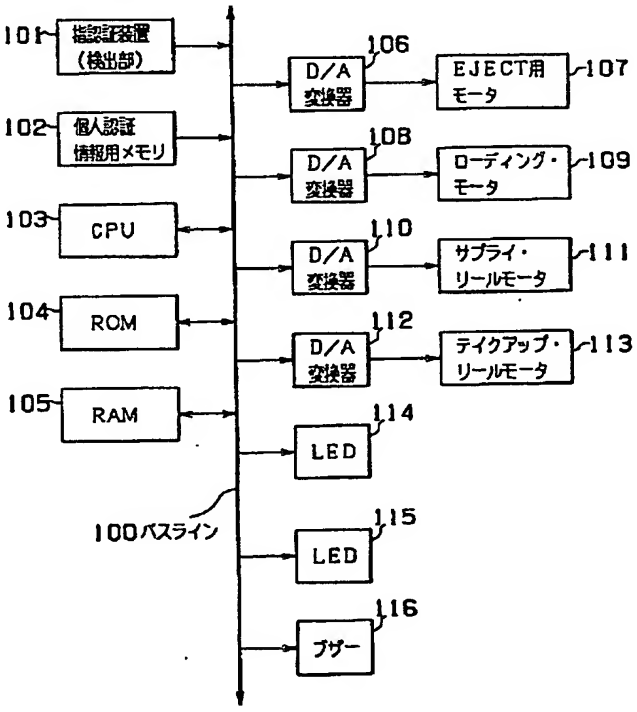
最終頁に続く

(54)【発明の名称】　生体情報を使用する記録再生装置及び記録再生方法

(57)【要約】

【課題】　記録再生装置および記録媒体に対して絶対的な所有権を確立し、著作権やプライバシー等を保護可能な、生体情報を使用する記録再生装置及び記録再生方法を提供するすること。

【解決手段】　指認証装置１０１は、その検出部により検出された生体情報と個人認証情報用メモリ１０２に記憶されている生体情報との照合を行い、被認証者の個人認証動作を行う。個人認証をパスすると、ＣＰＵ１０３は、記録再生装置の動作を許可し、カセットテープをローディングさせるモータ１０９やカセットをイジェクトさせるモータ１０７，テープ駆動を行うモータ１１１，１１３を動作可能な状態とする。一方、個人認証をパスしなかった場合、ＣＰＵ１０３は、記録再生装置の動作を許可せず、一切のモータ駆動を停止する。



【特許請求の範囲】
【請求項１】本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、
少なくとも１人分の生体情報を記憶する個人認証情報記憶手段と、
前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、
前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、
前記装置制限事項記憶手段に記憶された生体情報の登録，並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項管理手段と、
装置の動作状態を検出する装置動作検出手段と、
前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、
前記装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体とを具備したことを特徴とする生体情報を使用する記録再生装置。
【請求項２】前記生体情報検出手段は、皮膚の接触により生じる電気特性の変化に対応して、一次元の電気信号分布を形成する表面形状センサにより構成されることを特徴とする請求項１に記載の生体情報を使用する記録再生装置。
【請求項３】前記生体情報検出手段と前記装置動作検出手段とは、一体に形成されていることを特徴とする請求項１に記載の生体情報を使用する記録再生装置。
【請求項４】前記個人認証情報記憶手段，並びに装置制限事項記憶手段は、前記記録再生媒体上の所定のエリアに設けられていることを特徴とする請求項１に記載の生体情報を使用する記録再生装置。
【請求項５】前記生体情報検出手段は、皮膚の接触において、接触面の圧力を高める方向へ皮膚が移動することによって生体情報の検出が行われることを特徴とする請求項３に記載の生体情報を使用する記録再生装置。
【請求項６】前記生体情報検出手段は、自動または手動で移動する手段を備え、個人認証のための生体情報を検出する際に自動または手動で装置外部に移動し、個人認証後に自動または手動で装置内部に移動することを特徴とする請求項１に記載の生体情報を使用する記録再生装置。
【請求項７】本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、
前記生体情報を検出する方法により得られた生体情報と、少なくとも１人分の個人認証情報である生体情報を記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、
前記生体情報記憶手段に記憶された生体情報に対応して設定された、装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録，並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項を管理する方法と、
装置の動作状態を検出する方法と、
前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法とを具備したことを特徴とする生体情報を使用する記録再生方法。
【請求項８】本体またはリモコンに設けられ、生体情報を検出する第１の生体情報検出手段と、
少なくとも１人分の生体情報を記憶する第１の個人認証情報記憶手段と、
前記第１の生体情報検出手段により得られた生体情報と、前記第１の個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う第１の個人認証手段と、
前記第１の個人認証情報記憶手段に記憶される生体情報に対応して設定された装置の使用制限事項を記憶する第１の装置制限事項記憶手段と、
前記第１の装置制限事項記憶手段に記憶された生体情報の登録，並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録，変更，並びに削除を行う第１の装置制限事項管理手段と、
装置の動作状態を検出する第１の装置動作検出手段と、
前記第１の装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて、該装置の動作を制御する第１の装置動作制御手段と、
前記第１の装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録または再生動作が行われる第１の記録再生媒体とを備え、前記第１の個人認証情報記憶手段，並びに第１の装置制限事項記憶手段が、前記第１の記録再生媒体上の所定のエリアに設けられた第１の記録再生装置と、
本体またはリモコンに設けられ、生体情報を検出する第２の生体情報検出手段と、
少なくとも１人分の生体情報を記憶する第２の個人認証情報記憶手段と、
前記第２の生体情報検出手段により得られた生体情報

と、前記第２の個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う第２の個人認証手段と、
前記第２の個人認証情報記憶手段に記憶される生体情報に対応して設定された装置の使用制限事項を記憶する第２の装置制限事項記憶手段と、
前記第２の装置制限事項記憶手段に記憶された生体情報の登録，並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録，変更，並びに削除を行う第２の装置制限事項管理手段と、
装置の動作状態を検出する第２の装置動作検出手段と、
前記第２の装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて、該装置の動作を制御する第２の装置動作制御手段と、
前記第２の装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録または再生動作が行われる第２の記録再生媒体とを備え、前記第２の個人認証情報記憶手段，並びに第２の装置制限事項記憶手段が、前記第２の記録再生媒体上の所定のエリアに設けられた第２の記録再生装置と、
少なくとも前記第１または第２の記録再生装置の何れか一方に設けられた、前記第１および第２の記録媒体に記憶されている個人認証情報データを比較する個人認証情報データ比較手段と、
前記個人認証情報データ比較手段により比較した結果が一致した場合のみ、前記第１の記録再生装置からの再生情報が、前記第２の記録再生装置にてダビング記録可能とする手段とを具備したことを特徴とする生体情報を使用する記録再生装置。
【請求項９】本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する第１の方法と、
前記生体情報を検出する第１の方法により得られた生体情報と、少なくとも１人分の個人認証情報である生体情報を記憶する第１の生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う第１の方法と、
前記第１の生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する第１の装置使用制限事項記憶手段により記憶された、生体情報の登録，並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項を管理する第１の方法と、
装置の動作状態を検出する第１の方法と、
前記装置の動作状態を検出する第１の方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の第１の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する第１の方法とを備え、前記第１の個人認証情報記憶手段，並びに第１の装置制限事項記憶手段が、前記第１の記録再生媒体上の所定のエリアに設けられた第１の記録再生装置と、
本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する第２の方法と、
前記生体情報を検出する第２の方法により得られた生体情報と、少なくとも１人分の個人認証情報である生体情報を記憶する第２の生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う第２の方法と、
前記第２の生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する第２の装置使用制限事項記憶手段により記憶された、生体情報の登録，並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項を管理する第２の方法と、
装置の動作状態を検出する第２の方法と、
前記装置の動作状態を検出する第２の方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の第２の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する第２の方法とを備え、前記第２の個人認証情報記憶手段，並びに第２の装置制限事項記憶手段が、前記第２の記録再生媒体上の所定のエリアに設けられた第２の記録再生装置と、
少なくとも前記第１または第２の記録再生装置の何れか一方に設けられた、前記第１および第２の記録媒体に記憶されている個人認証情報データを比較する方法と、
前記個人認証情報データを比較する方法により比較した結果が一致した場合のみ、前記第１の記録再生装置からの再生情報が、前記第２の記録再生装置にてダビング記録可能とする方法とを具備したことを特徴とする生体情報を使用する記録再生方法。
【請求項１０】本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、
少なくとも１人分の生体情報を記憶する個人認証情報記憶手段と、
前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、
前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、
前記装置制限事項記憶手段に記憶された生体情報の登

録，並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項管理手段と、
装置の動作状態を検出する装置動作検出手段と、
前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、
前記装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体と前記個人認証情報記憶手段，並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、
暗号化またはスクランブルされた記録データを作成する手段と、
暗号化またはスクランブルされたデータを記録する際に、暗号化またはスクランブルを解くためのキーデータを、前記所定の個人認証情報を用いて作成する手段と、
前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを前記記録再生媒体に記録する手段とを具備したことを特徴とする生体情報を使用する記録再生装置。
【請求項１１】本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、
少なくとも１人分の生体情報を記憶する個人認証情報記憶手段と、
前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、
前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、
前記装置制限事項記憶手段に記憶された生体情報の登録，並びに削除、および生体情報に対応して設定された装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項管理手段と、
装置の動作状態を検出する装置動作検出手段と、
前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行い、その認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、
前記装置動作制御手段の制御により、映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体と前記個人認証情報記憶手段，並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、
暗号化またはスクランブルされた記録データを作成する手段と、
暗号化またはスクランブルされたデータを記録する際に、暗号化またはスクランブルを解くためのキーデータを、前記所定の個人認証情報を用いて作成する手段と、
前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを前記記録再生媒体に記録する手段と、
再生時に個人認証データを入力し、登録してある個人認証データと比較する比較手段と、
前記比較手段による比較結果が、一致していた場合のみ、前記記録媒体からキーデータを読み出し、読み出したキーデータに基づいて暗号を解く、またはデスクランブルする手段とを具備したことを特徴とする生体情報を使用する記録再生装置。
【請求項１２】本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、
前記生体情報を検出する方法により得られた生体情報と、少なくとも１人分の個人認証情報である生体情報を記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、
前記生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録，並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項を管理する方法と、
装置の動作状態を検出する方法と、
前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法と前記個人認証情報記憶手段，並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、
暗号化またはスクランブルされた記録データを作成する方法と、
暗号化またはスクランブルされた前記記録データを記録する際に、暗号化またはスクランブルを解くキーデータを、前記所定の個人認証データを用いて作成する方法と、
前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを記録媒体に記録する方法とを具備したことを特徴とする生体情報を使用する記録再生方法。
【請求項１３】本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、
前記生体情報を検出する方法により得られた生体情報と、少なくとも１人分の個人認証情報である生体情報を

記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、
前記生体情報記憶手段に記憶された生体情報に対応して設定され、装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録，並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項を管理する方法と、
装置の動作状態を検出する方法と、
前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法と前記個人認証情報記憶手段，並びに装置制限事項記憶手段を、前記記録再生媒体上の所定のエリアに形成する手段と、
暗号化またはスクランブルされた記録データを作成する方法と、
暗号化またはスクランブルされた前記記録データを記録する際に、暗号化またはスクランブルを解くキーデータを、前記所定の個人認証データを用いて作成する方法と、
前記所定の個人認証データを用いて作成した前記キーデータおよび前記暗号化またはスクランブルされた記録データを記録媒体に記録する方法と、
再生時に個人認証データを入力し、登録してある個人認証データと比較する方法と、
比較結果が一致していた場合にのみ、前記記録媒体からキーデータを読み出して、読み出したキーデータにもとづいて暗号を解く、またはデスクランブルする方法とを具備したことを特徴とする生体情報を使用する記録再生方法。
【請求項１４】前記リモコンは、
生体情報を検出する手段と、
被制御装置を選択する手段と、
被制御装置の機能を選択する手段と、
前記生体情報と被制御装置を選択する情報と被制御装置の機能を選択する情報を、被制御装置を制御する信号に変換する手段と、
前記被制御装置を制御する信号を出力する手段とを具備したことを特徴とする請求項１から６乃至８，１０，１１に記載の生体情報を使用する記録再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、映像，音声，またはディジタルデータ等を記録・再生する記録再生装置に係り、特に生体情報検出手段を有し、検出された生体情報に基づいて制御を為す、生体情報を使用する記録再生装置及び記録再生方法に関する。
【０００２】
【従来の技術】近年、情報化社会の高度化に伴い、個人または企業が取り扱う情報量、特に電子化された情報データ量は増加の一途をたどっている。これら情報データの多くは対外的に秘密保持を要するものが普通である。特に、情報の商品化が急速に進んだ現代においては、個人のプライバシーや企業秘密等の保護に加え、著作権等の保護などの様々な観点から、これら情報の扱いは非常に重要なものとなってきている。そのため、これら様々な情報、特にディジタル化された情報の漏洩や改ざん、或いは不正コピー等に対する防御方法（セキュリティシステム）が問われるようになってきている。
【０００３】ホストコンピュータやワークステーション等のネットワークや、早くから電算化されている金融関係のシステムでは、記録されている個人に関する情報やシステムの操作権（アクセス権）は厳重に守られており、暗証番号やパスワードといったキーワードや、光カードやＩＣカードを使用した物理的な施錠等が用いられている。
【０００４】このように、ネットワークを介してのプライバシーや著作権侵害等に関する保護対策は、かなりの水準にまで達しており、相当の成果をあげている。
【０００５】これに対し、ネットワークを介さないローカルなシステム、例えば、映像や音声情報等を扱う記録再生装置を基本とするシステムでは、著作権を無視した不正なコピー等が自由に行われ、国際的に問題化している。
【０００６】以下、図１７を参照しながら記録媒体としてテープ媒体を用いた従来の記録再生装置（ビデオテープレコーダ）について説明を行う。図１７は従来の記録再生装置の構成を示すブロック図である。
【０００７】図１７において、ビデオテープレコーダ（以下、ＶＴＲ）などの記録再生装置は、バスライン１００に接続されたＣＰＵ１０３がバスライン１００を介し、制御信号を各種モータ（１０７，１０９，１１１，１１３）に対して供給することによりメカ動作が行われる。ＣＰＵ１０３の制御プログラムはＲＯＭ１０４に格納されている。各モータは、対応する各Ｄ／Ａ変換器（１０６，１０８，１１０，１１２）にモータ動作に対応した制御信号が供給されることによりそれぞれ動作する。ＥＪＥＣＴ用モータ１０７は、挿入されている（ローディング状態にある）カセット（ビデオカセットテープ）を排出する動作を行うものである。ローディング・モータ１０９は、カセット挿入後、移動式テープガイトによりテープを所定の位置まで引き出し、図示しない回転ドラムヘッドにテープを巻き付けたり、カセットを排出する際、前記回転ドラムヘッドに巻き付いているテープをカセット内に巻き戻す動作を行うものである。サプライ・モータ１１１およびテイクアップ・リールモータ１１３は、それぞれ図示しないサプライリールおよびテ

イクアップリールを回転させてテープの巻き取りおよび送り出しを制御してテープ駆動動作を行うものである。

【０００８】以上の構成において、カセットをＶＴＲに挿入すると、ローディング・モータ１０９が動作して、自動的にテープが回転ドラムヘッドに巻き付けられる（テープローディングが為される）。この状態で、操作者がＶＴＲの再生ボタンを押下すると、サプライ・リールモータ１１１およびテイクアップ・リールモータ１１３が動作して、テープ駆動動作が行われ、テープの再生を行うことができる。また、操作者がＶＴＲの記録ボタンを押下すと、記録保護がなされていないカセットの場合、再生時と同様にサプライ・リールモータ１１１およびテイクアップ・リールモータ１１３が動作して、テープ駆動が行われ、テープに記録することができる。

【０００９】以上のように、従来の記録再生装置（ＶＴＲ）では、誰がＶＴＲを操作しようと、テープへの記録またはテープ再生を自由に行うことが可能である。尚、所有者情報（文字）をテープ中に画像情報として挿入・記録したり、テープ中の所定の領域にコンテンツ情報を挿入したり、或いは６mmディジタルカセットの場合には、カセットに設けられたＭＩＣ（ Memory In Cassette）と呼ばれるＩＣメモリ上に所有者およびコンテンツ情報を記録しておくことで、再生時、表示画面上にそれらの情報を表示させることにより、ＶＴＲ内に挿入されたカセットの所有者およびコンテンツ情報を操作者等に知らしめることは可能ではあるが、当該テープ（カセット）への記録またはテープ再生を自由に行うことは可能であり、物理的に操作不能状態とはならない。

【００１０】このように、上記従来の記録再生装置では、何れも所有者や著作権者の情報やコンテンツ情報を画面上に表示させるのみであり、記録媒体上に記録されている情報やシステムの操作権（アクセス権）の保護による、所有者や著作権者の権利保護は、一切為されない。即ち、上記従来の記録再生装置では、いわゆる著作物を自由にコピー（ダビング）し、複製を作成可能である。

【００１１】近年、技術の進歩に伴い、映像や音声情報等をほとんど劣化させることなく複製を容易に作成することが可能となっており、特に、ディジタル映像やディジタル音声情報等の場合、完全に同一な複製が作成可能であるため、早急な対策が求められている。

【００１２】さらに、上記従来の記録再生装置は、既述のコンピュータシステムと異なり、暗証番号やパスワードといったキーワードや、光カードやＩＣカードを使用した物理的な施錠機能を持たないため、第三者によるシステム（装置）の無断使用を防止する手段が無く、第三者により記録媒体への誤記録や誤消去が為される可能性を有すると共に、前記記録再生装置（ムービー等のポータブル機器）の盗難時等において、パーソナル映像や極秘映像（ビデオ撮影による記録映像等）のセキュリティー確保の手段が皆無である。

【００１３】

【発明が解決しようとする課題】上記の如く、従来の記録再生装置では、セキュリティー確保の手段を有しないため、所有者以外の人間が無断で装置を操作したり、他人のテープを自由に再生することが可能であり、個人（所有者）のプライバシーが保護されないという問題があった。さらには、無断で装置を操作する所有者以外の人間が、装置の操作を誤って、テープの誤記録や誤消去が為される可能性を有するなどの問題があった。

【００１４】そこで、本発明はこのような問題に鑑み、テープやディスクなどを記録媒体とする記録再生装置および記録媒体に対して絶対的な所有権を確立し、著作権やプライバシー等を保護すると共に、記録媒体への第三者による誤記録，誤消去を防止することが可能な、生体情報を使用する記録再生装置及び記録再生方法を提供することを目的とするものである。

【００１５】

【課題を解決するための手段】上記の目的を達成するために、本発明の記録再生装置は、本体またはリモコンに設けられ、生体情報を検出する生体情報検出手段と、少なくとも１人分の生体情報を記憶する個人認証情報記憶手段と、前記生体情報検出手段により得られた生体情報と、前記個人認証情報記憶手段に記憶された生体情報とを比較し、個人認証を行う個人認証手段と、前記個人認証情報記憶手段に記憶される生体情報に対応して設定された、装置の使用制限事項を記憶する装置制限事項記憶手段と、前記装置制限事項記憶手段に記憶された生体情報の登録，並びに削除、および生体情報に対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項管理手段と、装置の動作状態を検出する装置動作検出手段と、前記装置動作検出手段により検出された装置の動作状態に応じて個人認証を行いその認証結果および認証された生体情報の有する装置の使用制限事項に基づいて装置の動作を制御する装置動作制御手段と、前記装置動作制御手段の制御により映像情報や音声情報などの各種情報の記録、または再生動作が行われる記録再生媒体とを具備したことを特徴とするものである。

【００１６】また、本発明の記録再生方法は、本体またはリモコンに設けられ、皮膚の接触により生じる電気特性の変化に対応して一次元の電気信号分布を形成する表面形状センサによって、生体情報を検出する方法と、前記生体情報を検出する方法により得られた生体情報と、少なくとも１人分の個人認証情報である生体情報を記憶する生体情報記憶手段に記憶された生体情報とを比較して、個人認証を行う方法と、前記生体情報記憶手段に記憶された生体情報に対応して設定された装置の使用制限事項を記憶する装置使用制限事項記憶手段により記憶された、生体情報の登録，並びに削除、および生体情報に

対応して設定された、装置の使用制限事項の登録，変更，並びに削除を行う装置制限事項を管理する方法と、装置の動作状態を検出する方法と、前記装置の動作状態を検出する方法により検出された装置の動作状態に対応して個人認証を行い、その認証結果および認証された生体情報に対応して設定された装置の使用制限事項に基づいて、装置内の記録再生媒体に対して行われる、映像情報や音声情報などの各種情報の記録または再生のための動作を制御する方法とを具備したことを特徴とするものである。

【００１７】ここで、上記記載の発明によれば、記録再生装置を使用する際に個人認証が行われ、認証されたもののみが記録再生装置の使用を許される。また、認証には記録再生装置内に登録された個人認証情報が用いられ、認証情報として生体情報（指情報等）が用いられる。これにより、記録再生装置が盗難にあった場合など、正常に動作しない（第三者による操作不可能）ため盗難防止効果が得られる。また、個人使用（パーソナルユース）のための装置の場合、第三者による記録が出来ないため誤記録，誤消去を防ぐことができると共に、テープなどの媒体に記録されているパーソナル情報を保護することができる。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図１は本発明の実施の形態に係る生体情報による個人認証装置を具備した記録再生装置を示すブロック図である。

【００１９】本発明の実施の形態では、生体情報による個人認証装置として指認証装置を具備したビデオカセットテープを利用したムービーなどの記録再生装置を例に説明を行う。

【００２０】図１において、ビデオテープレコーダ（以下、ＶＴＲ）等の記録再生装置は、バスライン１００に接続されたＣＰＵ１０３がバスライン１００を介し、各種モータ（１０７，１０９，１１１，１１３）に対し、制御信号を供給することにより、メカの動作が行われるものである。ＣＰＵ１０３の制御プログラムはＲＯＭ１０４に格納されている。各モータは、対応する各Ｄ／Ａ変換器（１０６，１０８，１１０，１１２）に対し、モータ動作に対応した所定の制御信号が供給されることによりそれぞれ動作するものである。

【００２１】そして、ＥＪＥＣＴ用モータ１０７は、挿入されている（ローディング状態にある）カセット（ビデオカセットテープ）を排出する動作を行うものである。ローディング・モータ１０９は、カセット挿入後、移動式テープガイトによりテープを所定の位置まで引き出し、図示しない回転ドラムヘッドにテープを巻き付けたり、カセットを排出する際、前記回転ドラムヘッドに巻き付いているテープをカセット内に巻き戻す動作を行うものである。サプライ・モータ１１１およびテイクアップ・リールモータ１１３は、それぞれ図示しないサプライリールおよびテイクアップリールを回転させてテープの巻き取りおよび送り出しを制御してテープ駆動動作を行うものである。

【００２２】また、指認証装置（検出部）１０１は、例えば指を乗せることにより、あらかじめ個人認証情報用メモリ１０２に記憶されている情報に基づいて個人認証動作を行うものである。個人認証情報用メモリ１０２は、後述する登録モードにより個人認証情報の登録，変更並び削除等が行われる。尚、ＣＰＵ１０３は、前記装置のメカ動作（各モータ）の制御を行うと共に、個人認証のための演算処理動作を行う。そのための制御プログラムが前記ＲＯＭ１０４に格納されている。

【００２３】さらに、前記バスライン１００には、前記指認証装置（検出部）１０１やＣＰＵ１０３の動作状態をモニターするためのＬＥＤ１１４，１１５やブザー１１６が接続されている。

【００２４】次に、本発明の生体情報による個人認証装置を具備した記録再生装置の個人認証動作について、図２を参照しながら説明を行う。図２は個人認証動作手順を示したフローチャートである。

【００２５】上記の構成において、操作者（被認証者）により装置の電源が投入，またはカセットテープがＶＴＲに挿入されると、ＶＴＲ（本発明の生体情報による個人認証装置を具備した記録再生装置）は、個人認証動作を開始する（ステップＳ１，Ｓ２）。即ち、指認証装置１０１は、その検出部により検出された生体情報（指情報）と、個人認証情報用メモリ１０２に記憶されている生体情報（指情報）との照合を行い、被認証者がＶＴＲ（記録再生装置）に登録されている人物か否かの個人認証動作を行う。当然に、個人認証動作をパスしないと機器を動作させることはできない。個人認証動作のための手順（プログラム）はＲＯＭ１０４に格納されていて、フラッシュメモリやＩＣメモリ等の書き換え可能な個人認証情報用メモリ１０２に保存されている個人認証情報（指情報）をもとに、前記プログラムにしたがって、ＣＰＵ１０３により個人認証が行われる。

【００２６】指照合の結果、登録者であることが判明した場合、即ち指認証装置１０１の検出部により検出された生体情報（指情報）と、個人認証情報用メモリ１０２に記憶されている生体情報（指情報）とが一致し、被認証者が認証された場合、ＣＰＵ１０３は、ＶＴＲ（記録再生装置）の動作を許可し、これにより、メカ部、即ち、カセットテープをローディングさせるモータ１０９やカセットをイジェクトさせるモータ１０７，テープ駆動を行うモータ１１１，１１３を動作可能な状態となり（ステップＳ３，Ｓ４）、記録・再生などの通常動作を行うことが可能となる（ステップＳ５）。

【００２７】一方、前記指照合の結果、登録者でないと判別された場合、即ち指認証装置１０１の検出部により

検出された生体情報（指情報）と、個人認証情報用メモリ１０２に記憶されている生体情報（指情報）とが一致せず、被認証者が認証なかった場合、ＣＰＵ１０３は、ＶＴＲ（記録再生装置）の動作を許可せず、一切のモータ駆動を停止する（ステップＳ３，Ｓ６）。さらに、認証されなかった前記被認証者の指情報を個人認証情報用メモリ１０２に保存する（ステップＳ７）。これにより、正規登録者（ＶＴＲ装置の所有者等）は、不正にＶＴＲ（記録再生装置）を操作しようとした者を特定するための情報を得ることができる。

【００２８】本実施の形態では、記録媒体としてビデオカセットテープを使用するムービーを例に説明したが、これに限定されるものではなく、例えば、記録媒体がディスク状の物でも良いし、ＩＣメモリ状のものでも良い。また、モータ制御用と個人認証演算用のＣＰＵ，ＲＯＭ，並びにＲＡＭを、前記ＣＰＵ１０３，ＲＯＭ１０４，並びにＲＡＭ１０５の１セットで兼ねて（共用して）いるが、それぞれ別々の構成としても良い。さらに、個人認識のための生体情報として指情報を用いているが手や足，目など他の生体情報でも勿論良い。

【００２９】以上のように、生体情報によって個人認証を行い、認証されない場合、記録再生装置の動作を停止させる機能を設けたので、記録再生装置が盗難にあった場合でも、登録者（所有者等）以外によって、前記記録再生装置を正常に動作させることは不可能であり、これにより、前記記録再生装置の盗難を防止する効果を得られる。また、記録再生装置が個人専用の装置（パーソナルユース）として使用される場合、第三者による操作が不可であるため、誤記録，誤消去を防ぐことが出来ると共にテープ等の記録媒体に記録されているパーソナル情報を保護することができる。

【００３０】次に、本発明の記録再生装置の個人認証情報用メモリ１０２への認証情報（指情報）の登録および取り消し方法の一例について説明を行う。尚、本発明の記録再生装置には、スーパーユーザー登録モード／取り消しモード，および一般ユーザー登録モード／取り消しモードを有するものとして説明を行う。

【００３１】先ず、記録再生装置（以下、単に装置ともいう）の絶対使用者であるスーパーユーザーに関する登録モードについてであるが、原則、スーパーユーザーの登録は、例えば、装置の新規購入時などのスーパーユーザー未登録時においてただ１人のみ行うことができる。スーパーユーザーの登録を行おうとする者は、記録再生装置に設けられた図示しない操作手段によって、スーパーユーザー登録モードを選択し、指認証装置１０１の検出部に指を乗せる。すると、前記ＣＰＵ１０３は、指認証装置１０１により検出された個人認証情報（指情報）を、スーパーユーザーの個人認証情報（指情報）として個人認証情報用メモリ１０２に記憶し、これによりスーパーユーザーの登録が為される。

【００３２】次に、一般ユーザー登録モードについてであるが、一般ユーザーの登録は、スーパーユーザーにより認められた、記録再生装置の操作許可者（家族や友人など）についてのみ登録を行うことができる。このため、一般ユーザーの登録は、既述の個人認証動作に基づいて、指認証装置１０１によりスーパーユーザーが認証された後にのみ行うことができる。

【００３３】指認証装置１０１によりスーパーユーザーが認証され、記録再生装置が操作可能状態となった後、図示しない前記操作手段によって、一般ユーザー登録モードを選択し、指認証装置１０１の検出部に登録する一般ユーザーの指を乗せる。これにより、指認証装置１０１により検出された個人認証情報（指情報）は、一般ユーザーの個人認証情報（指情報）として個人認証情報用メモリ１０２に記憶され、一般ユーザーの登録が為される。尚、一般ユーザー登録モードになっている間は何人でも登録することができ、モードを解除すると登録モードは終了し、一般ユーザーの登録が終了する。また、上記登録において、指を一本だけ登録した場合、登録した指をケガした場合など、個人認証の際に、認識（認証）されないという可能性があるため、他の指を複数本同時に登録しておくと良い。

【００３４】次に、スーパーユーザーの登録取り消しモードについてであるが、スーパーユーザーの登録取り消しは、当然スーパーユーザーのみにより可能である。スーパーユーザー登録の取り消しは、スーパーユーザーが認証された後、前記記録再生装置に設けられた図示しない操作手段によりスーパーユーザー登録取り消しモードを選択し、スーパーユーザーが指認証装置（検出部）１０１に指を乗せる。これにより、指認証装置１０１により検出された個人認証情報（指情報）、即ち、被認証者と一致する個人認証情報（スーパーユーザーの指情報）が個人認証情報用メモリ１０２から消去され、これにより、スーパーユーザーの登録が取り消される。この際、一般ユーザー登録が為されていても、スーパーユーザーの登録が取り消されるのと同時に全て取り消される。

【００３５】次に、一般ユーザーの登録取り消しモードについてであるが、一般ユーザー登録の取り消しは、登録時と同様にスーパーユーザーが認証された後、前記図示しない操作手段により一般ユーザー登録取り消しモードを選択し、一般ユーザーが指認証装置（検出部）１０１に指を乗せる。これにより、指認証装置１０１により検出された個人認証情報（指情報）、即ち、被認証者と一致する個人認証情報（一般ユーザーの指情報）が個人認証情報用メモリ１０２から消去され、これにより、一般ユーザーの登録が取り消される。

【００３６】ところで、上記記録再生装置には、前記図１に示す如くに、ＬＥＤ１１４，１１５やブザー１１６などが設けられており、例えば上記被認証者を認証中（指認証装置（検出部）１０１に指が乗っている間）、

ＬＥＤ１１４を点灯させたりブザー１１６から音を発し、認証された場合、ＬＥＤ１１５を点灯させたり認証中とは異なる音色をブザー１１６から発することにより被認証者に装置が動作中（認証中）であることを知らせるようにしてもよい。これにより、認証状況を被認証者に容易に知らせることができる。尚、本実施の形態では、被認証者に装置が動作中（認証中）であることを知らせる方法の一例として、ＬＥＤとブザーを使用しているが、記録再生装置がムービー（ハンディーカメラー体型記録再生装置）などの場合には、ファインダー内のモニタ部に認証状況をマークやアイコン，或いは文字等を用いて表示するようにしても良いし、外部モニタに接続されている装置の場合は、認証状況を外部モニタに表示するようにしても良い。

【００３７】以上、個人認証情報および各個人認証情報毎に設定される装置に対する設定条件の対応付け（各個人毎の装置の使用制限）等を、記録再生装置の個人認証情報用メモリ１０２に登録し、これに基づいて、各個人に対する装置の使用制限を各記録再生装置毎で行う場合について説明したが、各個人に対する装置の使用制限を、各記録媒体毎に行うことも可能である。

【００３８】次に、個人認証情報および各個人認証情報毎に設定される装置に対する設定条件の対応付け（各個人毎の装置の使用制限）を、各記録媒体毎に行う場合について説明する。

【００３９】ここでは、民生用のディジタルＶＴＲを例に説明する。記録媒体への登録は、当該記録媒体に対して記録または再生を最初に行う者に対して最初の権利付与が行われる。例えば、未記録のカセットテープに記録を開始する際、個人認証が行われ、認証された個人認証情報および記録媒体に対する設定条件の対応付け（権利付与）が登録される。この後、他のユーザーの登録を行っても良い。尚、権利付与に関する登録内容としては、登録ユーザーの当該記録媒体の特定箇所への記録の許可／禁止，および再生の許可／禁止などである。

【００４０】また、再生専用のカセットテープ（記録媒体）の再生を最初に行う者に対しても同様の権利付与が行われる。即ち、当該記録媒体を初めて再生する際、個人認証が行われ、認証された個人認証情報および記録媒体に対する設定条件の対応付け（権利付与）が登録される。この後、同様に、他のユーザーの登録を行っても良い。権利付与に関する登録内容としては、登録ユーザーの当該記録媒体の特定箇所の再生の許可／禁止などである。

【００４１】前記権利付与に関する登録内容（カセットテープ毎の情報）は、カセットテープに埋め込まれたＲＡＭ（ＭＩＣ）に記録される。

【００４２】このようにして登録が行われたカセットテープが民生用のディジタルＶＴＲに挿入されると、ＶＴＲ（本発明の生体情報による個人認証装置を具備した記録再生装置）は、図１の指認証装置１０１の検出部により検出された生体情報（指情報）と、カセットテープに埋め込まれたＲＡＭ（ＭＩＣ）に記憶されている生体情報（指情報）との照合が行われ、被認証者が登録ユーザーか否かの個人認証が行われる。登録ユーザーであることが確認されると、確認（認識）されたユーザーの権利付与に関する登録内容が参照され、その登録内容にそった操作のみが許可され、実施可能となる。尚、前記被認証者が登録ユーザーか否かの個人認証（第２の認証）は、既述の記録再生装置自体に関する認証（第１の認証）をパスして、記録再生装置（民生用のディジタルＶＴＲ）の動作が可能な状態、即ち、記録・再生などの通常動作を行うことが可能な状態にて行われる。また、前記第１の認証と第２の認証は同時に行われても良いし、別々に行われても良い。

【００４３】前記カセットテープに埋め込まれたＲＡＭ（ＭＩＣ）に記録された前記権利付与に関する登録内容（カセットテープ毎の情報）の登録の変更および削除は、それぞれの設定の権利を持つ者が行うことができる。即ち、記録および再生の権利を有する者は記録および再生の何れの権利についても削除可能であり、再生のみの権利を有する者は再生の権利についてのみ削除可能である。尚、記録の権利を有する者も再生の権利を有する者もいない状態は、誰もが権利者になれる状態であり、未記録状態と同じ状態である。

【００４４】図３はメモリインカセットのメモリのデータストラクチャ例である。図３において、ＤＶＣ（民生用ディジタルＶＴＲ）の規格で決められたメインエリア２０１は、ＡＰＭ，ＢＣＩＤ，ＣＡＳＳＥＴＥ　ＩＤ，ＴＡＰＥ　ＬＥＮＧＴＨ，ＴＩＴＬＥ　ＥＮＤの各エリアにより構成される。

【００４５】また、オプショナルエリア２０２には、通常、タイトルなどテキストデータが記録される。本実施の形態では、指照合個人認証データと各個人毎の装置に対する設定条件がこのオプションエリアに記録される。ＭＩＣ（メモリインカセット）に記録されるシステムデータは、規格で、パック単位のデータストラクチャとなっており、１パックはヘッダー１バイトとデータ５バイトからなる。

【００４６】指照合個人認証データは精度によりデータ量が異なる。同様に、各個人毎の装置に対する設定条件もユーザーにより条件の数が異なる。このため、オプショナルエリア２０２には、同図に示すように、指照合個人認証データ（finger datalength）、個人毎の装置に対する設定条件データの全データ量（function datalength）それぞれについて、データ長を予め記録しておく。

【００４７】このような構成（フォーマット）とすることにより、メモリインカセットのメモリのデータストラクチャは、複数のシステムデータパックで構成されるこ

とになり、規格のＴＥＸＴデータの構造と同じになる。

【００４８】以上のようにカセットテープを管理することで、誤って他人の重要な情報を消去してしまったり、自己の重要な情報を他人に消去されることを未然に防止することができる。また、他人に見られたくないデータを自己以外の者に対しては再生不可とすることができ、プライバシーの保護が可能となる。さらに、カセットテープが盗難にあってもデータを再生される心配がない。

【００４９】ところで、上述の実施の形態では、個人認証情報または各個人毎の装置に対する設定条件を登録しておく箇所は、メモリ付きカセットのメモリであるとして説明を行ったが、これに限定する必要はない。

【００５０】即ち、テープ内の所定位置、例えば、サブコートやＶＡＵＸのシステムデータ記録エリアに、記録プログラム毎に登録データを記録することも可能である。この場合、図３で示した個人認証情報，または各個人毎の装置に対する設定条件のシステムデータパックをそのまま、サブコードやＶＡＵＸのオプショナルエリアに記録すればよい。

【００５１】また、個人認証情報または各個人毎の装置に対する設定条件を登録しておく箇所として、カセットに貼るラベルにバーコードで記録して、デッキ本体或いは専用装置がバーコードリードするようなシステムでもよい。

【００５２】さらには、インターフェースを本体或いはリモコンに有する記録再生装置として、ビデオテープレコーダ以外の、例えば、ＤＶＤ－ＲＡＭ（書き込み可能ディジタルビデオディスク）レコーダであってもよい。この場合、指照合個人認証データと各個人毎の装置に対する設定条件データを記録する箇所は、ＤＩＳＣのユーザーデータを記録する箇所であるＴＯＣ（ table of contents）部分とする。この場合、図７で示した指照合個人認証データおよび各個人毎の装置に対する設定条件データは、ＤＩＳＣのＴＯＣデータストラクチャに合わせて記録すればよい。

【００５３】次に、生体情報（指情報）を検出する、前記図１に示した指認証装置１０１について簡単に説明を行う。図４は本発明で個人認証を行うための生体情報検出手段として使用される指認証装置の一例を示すブロック図である。

【００５４】図４における指認証装置は、大きく分けて、指紋を入力するための指紋入力部１０（生体情報検出電極）と、この指紋入力部１０の出力に基づいて射影抽出（指紋情報）を求める射影計算部２０と、この射影計算部２０の出力に基づいてフィルタリング処理や照合計算を行なう信号処理部３０と、この信号処理部３０の出力に基づいてシステム制御，特徴登録，並びにＩ／Ｆ制御を行なう制御部４０とで構成されている。この場合、射影計算部２０～制御部４０までが個体認証部となる。

【００５５】図５は指紋入力部１０を構成する表面形状センサの具体的な構成を示す図である。図５において、基板３の表面には複数の線状接触子電極２（生体情報検出電極）が一次元のアレイ状に設けられている。また、各線状接触子電極２は電極取り出しパッド５に繋がっている。

【００５６】基板３の材料としては、例えば、ガラエポ等のプリント基板材料、セラミック板、あるいは絶縁被覆した金炉薄板などが用いられ、線状接触子電極２の材料としては、例えば、Ｃｕ薄膜、Ａｕ薄膜、Ｎｉメッキ薄膜、Ｐｔ薄膜，あるいはＰｄ薄膜等、人体或いは動物の皮膚から出る汗等の体液に侵されない導電性材料がもちいられる。

【００５７】また、線状接触子電極２の間隔は１／１０ｍｍ程度で構成され、線状接触子電極２の数、すなわち、電極アレイの長手方向の長さは、通常、指の先端から第２円関節を完全に含む程度の長さとなっている。

【００５８】このように構成された表面形状センサを有する指紋入力部１０によれば、線状接触子電極２に、指紋検出するべき指１が電極配列方向に対して直角方向に押し付けられると、隣接する線状接触子電極２で接触する指紋の凸部の量に応じて線状接触子電極２間の抵抗値が変化するので、一次元の抵抗分布が生じる。隣合う線状接触子電極２の間の指表面の抵抗値は、各電極取り出しパッド５から指１の長手方向に順次に読み取られる。

【００５９】図６は、指表面の抵抗値の測定原理を説明するための指紋入力部１０の等価画路である。

【００６０】図６において、ｉ＋１個の線状接触子電極２ｎ（１≦ｎ≦ｉ＋１）に対して指を押し付けたとき、隣接する線状接触子電極２ｎ，２ｎ＋１で接触する指紋の凸部の量に応じて線状接触子電極２間の抵抗値Ｒｎが変化する。隣接する二つの線状接触子電極２ｎ，２ｎ＋１の間に、図示の如く、基準抵抗Ｒｒｅｆと定電圧源Ｖｏとをアナログスイッチを介して接続する。このときの基準抵抗Ｒｒｅｆの両端の電位差Ｖｎは次式で与えられる。

【００６１】

$$Vn = Rref \cdot Vo / (Rref + Rn)$$

アナログスイッチを切り替えて、この電位差Ｖｎを指の長手方向に順次に読み取り、この電位差Ｖｎから算出された抵抗値Ｒｎを時系列にプロットすることにより、図７に示すように、指の長手方向への多値射影信号と等価な抵抗値で表現された指紋情報を得ることができる。

【００６２】なお、図７の横軸は隣接する線状接触子電極２ｎ，２ｎ＋１の位置を示しており、縦軸は抵抗他Ｒｎを示している。また、多チャンネルとなるので、アナログスイッチとしてアナログマルチプレクサＩＣを用いることにより、回路を小型化することができる。

【００６３】次に、以上のように構成された指認証装置

１０１の生体情報検出電極（線状接触子電極）２の記録再生装置への取付位置について説明を行う。図８および図９は生体情報検出電極２が一体に形成された本発明に係る記録再生装置のスイッチキー（操作ボタン）を示した図である。

【００６４】図８において、図８(a)はスイッチが押されていない状態を、図８(b)は指がスイッチを押している状態をそれぞれ示している。生体情報検出電極３０１はスイッチキー３０２の上面に配置され、支点３０３はスイッチキー３０２の手前（左側）に配置されている。

【００６５】以上の構成において、スイッチ３０４を操作（押下）するために、キー３０２を指３０５で押すと、キー３０２の前方部分が押し下げられスイッチ３０４が押下されると共に、指３０５の腹部全体に力がかかることにより、指３０５の腹部が生体情報検出電極３０１に圧着されることになる。これにより、指認証装置１０１は、確実に生体情報を読み取ることができ、個人認証動作を行うことができる。

【００６６】同様に、図９は、指３０５がスイッチキー４０２を引いている状態を示している。スイッチキー４０２には、垂直もしくは斜めに傾けて生体情報検出電極３０１が設けられている。

【００６７】以上の構成において、スイッチ４０３を操作（押下）するために、指３０５の腹部にて、スイッチキー４０２を手前に引く（矢印方向にスライドさせる）ことにより、スイッチ４０３が押下される。このとき、指３０５の腹部全体に力がかかり、指３０５の腹部が生体情報検出電極３０１に圧着される。これにより、指認証装置１０１は、確実に生体情報を読み取ることができ、個人認証動作を行うことができる。

【００６８】以上のようなスイッチ、即ち、スイッチ操作を行う際に必ず指３０５の腹部が生体情報検出電極３０１に圧着されるように構成されたスイッチを用いることにより、ユーザーは、個人認証が行われていることを意識することなく（気にすることなく）、記録再生装置の操作を行うことができる。

【００６９】以上、ユーザーに対して、個人認証が行われていることをできるだけ意識させないようにユーザー（装置使用者）の生体情報を取得する方法（スイッチの構成）について説明したが（ムービー等の小型の装置に有効）、次に、本発明に係る記録再生装置に対して所定の操作を行おうとした際に、装置により個人認証の必要が明示的に示され、この要求に従ってユーザー（装置使用者）が個人認証を意識的に受ける場合、即ち、ユーザーに生体情報の提供を要求することにより（ユーザーに認識させて）生体情報を取得する方法について説明を行う。

【００７０】図１０および図１１は本発明に係る生体情報による個人認証装置を具備した記録再生装置の一例を示す図である。

【００７１】図１０において、図１０(a)はスライドテーブル５０１が格納されている状態を示していて、図１０(b)はスライドテーブルが引き出されている状態をそれぞれ示している。

【００７２】本発明に係る記録再生装置（デッキ本体５０３）は、認証が必要になったときに、自動若しくは手動にて引き出されるスライドテーブル５０１を有し、スライドテーブル５０１上には生体情報検出電極３０１が設けられている。この生体情報検出電極３０１上に指の腹部を乗せることにより、ユーザー（操作者）の生体情報が読み取られ、この生体情報に基づいて個人認証が行われる。個人認証終了後、生体情報検出電極３０１は、自動若しくは手動にて、デッキ本体５０３内部に収納される。

【００７３】ユーザー（装置使用者）認証は、図示しない記録媒体をデッキ本体５０３に挿入した場合や、ユーザーが所定の操作を行おうとして操作キー等を押下した場合などに、自動的に生体情報検出電極が現れる、個人認証の必要が明示的に示される。前述の通り、生体情報検出電極３０１上に指の腹部を乗せ、個人認証が行われ、認証が完了すると格納される。これにより、異物等の付着による生体情報検出電極３０１の汚染を防ぎ得る。

【００７４】同様に、図１１において、図１１(a)はパネルドア６０２が格納されている状態を示していて、図１１(b)はパネルドア６０２が開いている状態をそれぞれ示している。尚、図１１は図１０の他の例を示したものである。

【００７５】本発明に係る記録再生装置（デッキ本体６０４）は、認証が必要になったときに、自動若しくは手動にて支点６０１をドア下部に持ち、手前に倒れるように開くパネルドア６０２の内側に引き出されるパネルドア６０２が設けられている。パネルドア６０２上には、生体情報検出電極３０１が配置されていて、この生体情報検出電極３０１上に指の腹部を乗せることにより、ユーザー（操作者）の生体情報が読み取られ、この生体情報に基づいて個人認証が行われ、個人認証終了後、パネルドア６０２は、自動若しくは手動にて、デッキ本体６０４内部に収納される。

【００７６】ユーザー（装置使用者）認証は、図示しない記録媒体をデッキ本体６０４に挿入した場合や、ユーザーが所定の操作を行おうとして操作キー等を押下した場合などに、自動的に生体情報検出電極３０１が現れ、個人認証の必要が明示的に示される。前述の通り、生体情報検出電極３０１上に指の腹部を乗せ、個人認証が行われ、認証が完了すると格納される。これにより、異物等の付着による生体情報検出電極３０１の汚染を図１０に示した場合と同様に防ぎ得る。

【００７７】以上、生体情報検出手段である指認証装置により検出された生体情報と、記録再生装置に設けられ

た記憶手段または記録再生装置で使用する記録媒体に登録された指照合個人認証データとにより個人認証を行い、その結果に基づいて、当該記録再生装置で使用する記録媒体への記録や再生の制限を行う、本発明である生体情報による個人認証装置を具備した記録再生装置について説明したが、次に、これら本発明による複数の記録再生装置間における記録データの複写（ダビング）制御（制限）について説明を行う。

【００７８】ここでは、上記個人認証情報および各個人毎の装置に対する設定条件が登録されている記録媒体、即ち、指照合個人認証データおよびそれらに対応した権利付与内容が登録されている記録媒体を第１の記録再生装置（再生側装置）により再生し、第２の記録再生装置（記録側装置）にて記録（ダビング）する場合について、図１２および図１３を参照しながら説明する。

【００７９】図１２は再生側装置および記録側装置の構成を示すブロック図であり、図１３はダビング動作を示したフローチャートである。

【００８０】図１２において、再生側装置７０２ａは、例えば、ＤＶＣ（民生用ディジタルＶＴＲ）等の個人認証データおよび各個人毎の装置に対する設定条件データが登録された記録媒体７０１ａと、個人認証データおよび各個人毎の装置の設定条件データ読み取り手段７０４ａと、個人認証データー致比較手段７０５ａと、ダビング許可禁止判定手段７０６ａと、記録再生制御手段７０３ａと、ケーブル７０８を介して記録側装置７０２ｂとデータのやりとりを行うディジタルインターフェース手段７０７ａと、により構成される。

【００８１】個人認証データおよび各個人毎の装置の設定条件データ読み取り手段７０４ａは、記録媒体７０１ａより個人認証データおよび各個人毎の装置に対する設定条件データを読み取る。個人認証データー致比較手段７０５ａは、ケーブル７０８よりディジタルインターフェース手段７０７ａを介して記録側装置７０２ｂより供給される個人認証データおよび各個人毎の装置に対する設定条件データと、前記読み取り手段７０４ａからの個人認証データおよび各個人毎の装置に対する設定条件データと、を比較する。ダビング許可禁止判定手段７０６ａは、個人認証データー致比較手段７０５ａの比較結果に基づいてダビングの許可または禁止を判定してその結果を出力する。記録再生制御手段７０３ａは、ダビング許可禁止判定手段７０６ａの判定結果に基づいて前記記録媒体７０１ａに対する再生の制御を行う。

【００８２】同様に、記録側装置７０２ｂは、例えば、ＤＶＣ（民生用ディジタルＶＴＲ）等の個人認証データおよび各個人毎の装置に対する設定条件データが登録された記録媒体７０１ｂと、個人認証データおよび各個人毎の装置の設定条件データ読み取り手段７０４ｂと、個人認証データー致比較手段７０５ｂと、ダビング許可禁止判定手段７０６ｂと、記録再生制御手段７０３ｂと、ケーブル７０８を介して再生側装置７０２ａとデータのやりとりを行うディジタルインターフェース手段７０７ｂと、により構成される。

【００８３】個人認証データおよび各個人毎の装置の設定条件データ読み取り手段７０４ｂは、記録媒体７０１ｂより個人認証データおよび各個人毎の装置に対する設定条件データを読み取る。個人認証データー致比較手段７０５ｂは、ケーブル７０８よりディジタルインターフェース手段７０７ｂを介して再生側装置７０２ａより供給される個人認証データおよび各個人毎の装置に対する設定条件データと、前記読み取り手段７０４ｂからの個人認証データおよび各個人毎の装置に対する設定条件データと、を比較する。ダビング許可禁止判定手段７０６ｂは、個人認証データー致比較手段７０５ｂの比較結果に基づいてダビングの許可または禁止を判定してその結果を出力する。記録再生制御手段７０３ｂは、ダビング許可禁止判定手段７０６ｂの判定結果に基づいて前記記録媒体７０１ｂに対する記録の制御を行う。

【００８４】以上の構成において、記録再生装置間は、例えばＩＥＥＥ１３９４などのインターフェース（ケーブル７０８，ディジタルインターフェース手段７０７ａ，７０７ｂ）を介してダビング可能な状態であるとする。ユーザーがダビングをしたい場合、例えば、再生側で再生キーを押下すると共に記録側でＲＥＣキーを押下するか、外部コントローラからダビングコマンドを出力（送信）する。何れの場合でも、ＩＥＥＥ１３９４等を介し、相手装置の（再生側装置は記録側装置の、記録側装置は再生側装置の）動作コマンドを知ることができ、ユーザーからダビング要求が有ったことを知ることができる（ステップＴ１）。

【００８５】記録側再生側それぞれの装置においてダビング要求が確認されると、再生側装置７０２ａ並びに記録側装置７０２ｂは、それぞれ個人認証データが記録されている記録媒体（例えば、メモリ付きカセット）から、個人認証データ，およびその個人の装置の設定条件データを読みとる（ステップＴ２，Ｔ３）。そして、再生側装置７０２ａは記録側装置７０２ｂで読みとった上記個人認証データ（およびその設定条件データ）をＩＥＥＥ１３９４等のディジタルインターフェースを介して再生側装置７０２ａへ伝送する。尚、逆に再生側装置７０２ａで読みとったデータを記録側装置７０２ｂに伝送してもよい（ステップＴ４）。

【００８６】さらに、再生側装置７０２ａは、前記読みとった個人認証データ（およびその設定条件データ）と、伝送された記録側装置７０２ｂの個人認証データとを、個人認証データー致比較手段７０５ａで比較する。一致していなければ、記録テープと再生テープとは、それぞれ別の人の所有であると推定され、ダビング許可禁止判定手段７０６ａによりダビング禁止の判定が為され、相手側装置（記録側装置）にダビング禁止信号をデ

ィジタルインターフェース手段７０７ａ，ＩＥＥＥ１３９４ケーブル７０８，およびディジタルインターフェース手段７０７ｂを介して伝送すると共にダビング動作を停止（禁止）する（ステップＴ５，Ｔ１０，Ｔ１１）。

【００８７】前記個人認証データー致比較手段７０５ａでの比較結果が一致していた場合には、再生側装置７０２ａで認証された個人の装置設定条件に「ＰＬＡＹ」はあるか、即ち、再生する権利を有するか（ステップＴ６）、また、記録側装置７０２ｂで認証された個人の装置設定条件に「ＲＥＣ」はあるか、即ち、記録する権利を有するか（ステップＴ７）が判定され、何れか一方でも満たさない（権利を有しない）場合には、ダビング動作を停止（禁止）する（ステップＴ１０，Ｔ１１）。

【００８８】前記ステップＴ６，Ｔ７が共に条件を満たす場合には、ダビング許可禁止判定手段７０６ａにより、ダビング許可の判定が為され、相手側装置（記録側装置）にダビング許可信号が、ディジタルインターフェース手段７０７ａ，ＩＥＥＥ１３９４ケーブル７０８，およびディジタルインターフェース手段７０７ｂを介して伝送されると共に、記録再生制御手段７０３ａ，７０３ｂによりダビング動作が開始される（ステップＴ８，Ｔ９）。

【００８９】なお、上記ステップＴ５，Ｔ６，Ｔ７の判定処理は、再生側装置７０２ａの個人認証データー致比較手段７０５ａおよびダビング許可禁止判定手段７０６ａによって行われるとして説明したが、記録側装置７０２ｂの個人認証データー致比較手段７０５ｂおよびダビング許可禁止判定手段７０６ｂにて行うようにしても良い。

【００９０】また、上記ダビング動作時には、記録媒体のデータのみコピーして、個人認証データや装置の設定条件等の記録は、原則コピーしないようにすることが望ましい。よって、本発明による個人認証データや装置の設定条件のデータを記録する記録媒体のデータをダビングする際、個人認証データや装置の設定条件を記録するデータは、全ての条件で、ダビングを禁止とする。

【００９１】さらに、以上の個人認証データおよび装置の設定条件のデータを用いたダビング許可禁止動作は、前述のＶＴＲのメモリ付きカセットに記憶した場合だけでなく、ＤＶＤ－ＲＡＭ　ＤＩＳＣのＴＯＣ部分など、他の記録再生装置の記録媒体の特定箇所の場合でも全て当てはまる。

【００９２】ところで、著作権侵害や不正コピー防止機能として、記録データを暗号化したりスクランブルをかけて記録するシステムが考案されていることは周知である。そこで、本発明の生体情報（個人認証データ）を、記録データを前記暗号化したりスクランブルをかけたり、あるいは暗号やスクランブルを解くためのキーとして使用することが考えられる。この方法を用いることにより、データの秘話性効果を格段に高めることが可能となる。以下、これについて説明を行う。

【００９３】本発明の記録再生装置、または記録媒体に、生体情報（個人認証データ）の登録の為されたユーザーの個人認証データ、或いは認証データに所定の演算を施したものを用いて（初期値として）、暗号やスクランブルのキーデータを発生させる。そして、このキーデータを用いてデータを暗号化、またはスクランブル化して、前記記録データを前記記録媒体に記録するようにする。尚、このキーデータ自体を記録媒体に記憶させておくことで、繰り返し再生を行うときなど、再生の度に、毎回、暗号やスクランブルのキーデータを発生（生成）する処理を省くことができる。

【００９４】次に、既述の如く本発明の記録再生装置から個人認証データを入力し（個人認証を行い）、登録してある個人認証データと比較し、比較結果が一致していた場合にのみ再生動作が行われる。再生動作は、例えば、前記記録媒体から記録時に記録されていたキーデータを読み出し、読み出したキーデータに基づいて、同じく前記記録媒体から読み出された暗号化（符号化）またはスクランブル化された記録データに復号またはデスクランブル処理が施され、これにより復元された記録データが得られる。

【００９５】以上により、秘話性が非常に高い記録再生装置を実現することができる。尚、暗号化（符号化）またはスクランブル化された記録データを前記記録媒体に記録する際、暗号化（符号化）またはスクランブル化のためのキーデータを前記記録媒体に記憶させておかなくても、再生時に、個人認証データからキーデータを発生し、このキーデータに基づいて、記録媒体から読み出された暗号化（符号化）またはスクランブル化された記録データに復号またはデスクランブル処理を施すことにより、復元された記録データが得られ、同様に、秘話性の非常に高い記録再生装置を実現することができることはいうまでもない。

【００９６】次に、生体情報検出電極をリモコン装置に設けた本発明の生体情報を使用する記録再生装置について説明を行う。図１４は本発明の実施の形態に係る生体情報検出電極を具備したリモコン装置を示すブロック図である。

【００９７】図１４（ａ）はリモコン装置の形態の一例を示したもので、リモコン８０１の表側には機能選択スイッチ８０３が複数配置されており、裏側には指を押しつけて電気抵抗を検出する生体情報検出電極３０１が設置されている。

【００９８】図１４（ｂ）は生体情報検出電極をリモコン装置に設けたＶＴＲ装置の構成を示したものである。リモコン８０１は、指を押しつけて電気抵抗を検出する前記生体情報検出電極３０１と、前記電気抵抗を指全体の１次元パターンに変換するパターン入力部８０６と、機能選択スイッチ８０３で選択された機能に対応する機

能選択信号を出力する機能選択部８０４と、パターン入力部８０６の出力と機能選択部８０４の出力とから、例えば図１４（ｃ）に示す如くの少なくとも指の１次元パターンのコード，並びに機能選択コードの２つの情報を伝達するための領域を有するデータフォーマットから成る、リモコンコード信号を出力するリモコンコード生成部８０５と、リモコンコード信号を赤外線などの送信信号に変換して出力する送信部８０７とから構成される。

【００９９】また、ＶＴＲ８１２は、前記送信信号を受信して前記リモコンコード信号に変換して出力する受信部８０８と、リモコンコード信号をデコードするリモコンコードデコード部８０９と、個人認証を行う個人認証処理部８１０と、ＶＴＲ装置の記録、再生等の動作の許可または禁止処理を行う制御部８１１とから構成される。

【０１００】次に、以上のように構成された生体情報検出電極をリモコン装置に設けたＶＴＲ装置の動作について説明を行う。

【０１０１】先ず、リモコン８０１の表側の機能選択スイッチ８０３が押下されると、機能選択部８０４で、前記各スイッチの機能に対応した機能選択信号を発生し、リモコンコード生成部８０５に出力する。一方、パターン入力部８０６では、リモコン裏側の生体情報検出電極３０１に指が押しつけられると、生体情報検出電極３０１で検出された電気抵抗値を、指全体の１次元パターン（以下、単に指の１次元パターンという）に変換し、前記リモコンコード生成部８０５に出力する。

【０１０２】リモコンコード生成部８０５では、パターン入力部８０６より指の１次元パターンが入力されている場合には、この指の１次元パターンと、機能選択部８０４から入力された機能選択信号とを、例えば図１４（ｃ）に示す如くのデータフォーマットにて、リモコンコード信号に変換し、送信部８０７に出力する。一方、パターン入力部８０６より指の１次元パターンが入力されていない場合には、リモコンコード信号の出力を行わない。

【０１０３】送信部８０７では、パターン入力部８０６よりリモコンコード生成部８０５に指の１次元パターンが入力されている場合に限り、リモコンコード生成部８０５から入力されたリモコンコード信号を、赤外線などの送信信号に変換して出力する。

【０１０４】ＶＴＲ８１２では、受信部８０８にて、前記リモコン８０１からの送信信号を受信する。受信部８０８で受信された信号は、例えば図１４（ｃ）に示す如くのデータフォーマットから成るリモコンコードに変換され、リモコンコードデコード部８０９に出力される。リモコンコードデコード部８０９では、受信部８０８より入力されたリモコンコード信号をデコードし、指の１次元パターンを個人認証処理部８１０へ出力すると共に、機能選択信号を制御部８１１に出力する。

【０１０５】個人認証処理部８１０では、リモコンコードデコード部８０９より入力された指の１次元パターンと、図示しない個人認証情報用メモリ１０２に登録された個人認証情報（指情報），または図示しない記録媒体であるカセットテープのＭＩＣやＤＶＤ－ＲＡＭのＴＯＣ等に登録された個人認証情報（および各個人毎の装置に対する設定条件データ）とから、個人認証処理を行い、その結果を制御部８１１へ出力する。

【０１０６】制御部８１１では、個人認証処理部８１０より供給された個人認証処理結果とリモコンコードデコード部８０９より供給された機能選択信号に従って、図２および図３で説明した如くに、即ち、前記個人認証処理部８１０より個人認証がパスしない場合には、記録，再生等のＶＴＲ８１２に対する一切の操作が禁止されて、個人認証をパスした場合には、前記図示しない記録媒体に登録された各個人毎の装置に対する設定条件データの内の、個人認証された者の装置に対する設定条件データの登録内容（認証された者が有する記録や再生等を行う権利）に基づいて、ＶＴＲ８１２に対する記録，再生等の動作が為される。

【０１０７】なお、前記記録媒体への新たな登録は、勿論、このリモコン装置を用いて行っても良いし、ＶＴＲ装置で行っても良い。

【０１０８】さて、上述のリモコン装置は、前記指全体の１次元パターンと機能選択信号共に揃ったとき、即ち、リモコンコード生成部８０５で、図１４（ｃ）に示す如くのデータフォーマットにて、リモコンコード信号が生成（変換）されることにより、送信部８０７を介してＶＴＲ８１２に出力される。リモコンコード信号の生成は、例えば、図１５（ａ）および図１５（ｂ）に示す２通りの手順により、リモコンコード生成部８０５にて行われる。以下、リモコンコード信号の生成手順について図１５を参照しながら説明を行う。図１５はリモコンコード信号の生成手順の２つの例を示すフローチャートである。尚、以下の手順では、認証処理は無条件でパスするものとする。

【０１０９】リモコンコード信号の生成例、即ち、図１５（ａ）に示す例の場合、リモコンコード生成部８０５では、以下の手順にて機能選択信号と指全体の１次元パターンの入力を受け付け、リモコンコードを生成出力する。

【０１１０】先ず、リモコンコード生成部８０５は、リモコン８０１の機能選択スイッチ８０３が押下されることにより、機能選択信号が入力されると、生体情報検出電極３０１に指が押しつけられることにより検出された電気抵抗値に基づいて、パターン入力部８０６により変換出力される、指全体の１次元パターンの入力待ち状態となる（ステップＵ１，Ｕ２，Ｕ３）。

【０１１１】そして、生体情報検出電極３０１に指が押しつけられると、パターン入力部８０６は、生体情報検

出電極３０１により検出された電気抵抗値に基づいて指全体の１次元パターンをリモコンコード生成部８０５に出力する（ステップＵ４，Ｕ５）。

【０１１２】これにより、リモコンコード生成部８０５は、例えば、前記図１４（ｃ）に示す如くのデータフォーマットにてリモコンコード信号を生成（変換）・出力し（ステップＵ６）、送信部８０７を介し、赤外線などの送信信号として、例えばＶＴＲ８１２に送信する。

【０１１３】次に、リモコンコード信号の他の生成例、即ち、図１５（ｂ）について説明を行う。図１５（ｂ）に示す例の場合、リモコンコード生成部８０５では、以下の手順にて機能選択信号と指全体の１次元パターンの入力を受け付け、リモコンコードを生成出力する。

【０１１４】先ず、リモコンコード生成部８０５は、リモコン８０１の生体情報検出電極３０１より指全体の１次元パターンの入力があると、機能選択スイッチ８０３の押下待ち状態、即ち、機能選択部８０４が発生する機能選択信号の入力待ち状態となる（ステップＶ１，Ｖ２，Ｖ３）。

【０１１５】そして、リモコン８０１の機能選択スイッチ８０３が押下されることにより、機能選択信号が入力されると、リモコンコード生成部８０５は、前記生体情報検出電極３０１より、継続して指全体の１次元パターンの入力があるか否か（指全体の１次元パターン入力が完了したか否か）の判別を行う。

【０１１６】リモコンコード生成部８０５は、継続して指全体の１次元パターンの入力がある場合には、例えば、前記図１４（ｃ）に示す如くのデータフォーマットにてリモコンコード信号を生成（変換）・出力し（ステップＶ６）、送信部８０７を介し、赤外線などの送信信号として、例えばＶＴＲ８１２に送信する。一方、継続して指全体の１次元パターンの入力がない（機能選択信号が入力されたタイミングに指全体の１次元パターンの入力がない）場合には、ステップＶ１にもどり、リモコン８０１の生体情報検出電極３０１より指全体の１次元パターンの入力待ち状態となる。

【０１１７】ところで、上記図１５（ａ）と図１５（ｂ）に示すそれぞれの場合の違いとして、例えば、図１５（ｂ）の場合には、機能選択信号と指全体の１次元パターンの入力が、リモコンコード生成部８０５に対してほぼ同時に行われる必要があるのに対し、図１５（ａ）の場合には、必ずしも同時である必要はない点が挙げられる。尚、送信信号出力後のＶＴＲ８１２の動作は、前記図１４で説明したＶＴＲ８１２の動作説明と同様であるので省略する。

【０１１８】次に、同時に複数の装置の操作が可能な、いわゆるマルチリモコン装置であって、上記図１４および図１５で説明した機能を有するリモコン装置について説明を行う。

【０１１９】図１６は本発明の実施の形態に係る生体情報検出電極を具備したマルチリモコン装置および被制御装置を示すブロック図である。

【０１２０】図１６（ａ）は生体情報検出電極を備えたマルチリモコン装置と被制御装置として、例えばテレビジョン受像機とＶＴＲ装置との構成を示したものである。リモコン８０１は、指を押しつけることにより電気抵抗を検出する生体情報検出電極３０１と、前記電気抵抗を指全体の１次元パターンに変換するパターン入力部８０６と、機能選択スイッチ８０３で選択された機能に対応する機能選択信号を出力する機能選択部８０４と、パターン入力部８０６の出力と機能選択部８０４の出力とから、例えば図１６（ｃ）に示す如くの少なくとも、装置選択コード，指の１次元パターンのコード，並びに機能選択コードの３つの情報を伝達するための領域を有するデータフォーマットから成るリモコンコード信号を出力するリモコンコード生成部８０５と、リモコンコード信号を赤外線などの送信信号に変換して出力する送信部８０７とから構成される。

【０１２１】また、テレビ８１３は、前記送信信号を受信して前記リモコンコード信号に変換して出力する受信部８０８と、リモコンコード信号をデコードするリモコンコードデコード部８１５と、前記リモコンコード信号より生成（デコード）された装置選択信号および機能選択信号に基づいてテレビジョン受像機の各種動作を制御する制御部８１６とから構成される。

【０１２２】さらに、ＶＴＲ８１４は、前記送信信号を受信して前記リモコンコード信号に変換して出力する受信部８０８と、リモコンコード信号をデコードするリモコンコードデコード部８１７と、個人認証を行う個人認証処理部８１８と、前記リモコンコード信号より生成（デコード）された装置選択信号および機能選択信号と前記個人認証処理部８１８からの出力信号に基づいて、ＶＴＲ装置の記録、再生等の動作の許可または禁止処理を行う制御部８１１とから構成される。

【０１２３】図１６（ｂ）はリモコン装置の形態の一例を示したもので、リモコン８０１の表側には、例えば、ＴＶ用とＶＴＲ用の機能選択スイッチ８０３が複数配置されており、裏側には指を押しつけて電気抵抗を検出する図示しない生体情報検出電極３０１が設置されている。

【０１２４】次に、以上のように構成された生体情報検出電極を具備したマルチリモコン装置および被制御装置であるテレビジョン受像機およびＶＴＲ装置の動作について説明を行う。

【０１２５】先ず、リモコン８０１の表側の機能選択スイッチ８０３が押下されると、機能選択部８０４で、前記各スイッチの機能に対応した機能選択信号を発生し、リモコンコード生成部８０５に出力する。一方、パターン入力部８０６では、リモコン裏側の生体情報検出電極３０１に指が押しつけられると、生体情報検出電極３０

１で検出された電気抵抗値を、指の１次元パターン（指全体の１次元パターン）に変換し、前記リモコンコード生成部８０５に出力する。

【０１２６】リモコンコード生成部８０５では、パターン入力部８０６より指の１次元パターンが入力されている場合には、この指の１次元パターンと、機能選択部８０４から入力された装置選択信号と機能選択信号とを、例えば図１６（ｃ）に示す如くのデータフォーマットにて、リモコンコード信号に変換し、送信部８０７に出力する。尚、パターン入力部８０６より指の１次元パターンが入力されていない場合には、リモコンコード信号の出力は行われない。

【０１２７】送信部８０７では、リモコンコード生成部８０５から入力されたリモコンコード信号を、赤外線などの送信信号に変換して出力する。

【０１２８】一方、ＶＴＲ８１４およびテレビ８１３などの装置では、リモコン８０１より出力された送信信号を受信部８０８で受信する。受信部８０８では、受信した信号を例えば図１６（ｃ）に示す如くのデータフォーマットのリモコンコード信号に変換する。

【０１２９】これ以後の処理は、個人認証を行う装置と個人認証を行わない装置（本実施の形態ではＶＴＲ８１４とテレビ８１３）で処理内容が異なる。

【０１３０】即ち、個人認証を行う装置であるＶＴＲ８１４では、受信部８０８にて、前記リモコン８０１からの送信信号を受信する。受信部８０８で受信された信号は、例えば図１６（ｃ）に示す如くのデータフォーマットから成るリモコンコードに変換され、リモコンコードデコード部８１７に出力される。リモコンコードデコード部８１７では、受信部８０８より入力されたリモコンコード信号をデコードし、指の１次元パターンを個人認証処理部８１８へ出力すると共に、装置選択信号および機能選択信号を制御部８１９に出力する。

【０１３１】個人認証処理部８１８では、リモコンコードデコード部８１７より入力された指の１次元パターンと、図示しない個人認証情報用メモリに登録された個人認証情報（指情報），または図示しない記録媒体であるカセットテープのＭＩＣやＤＶＤ－ＲＡＭのＴＯＣ等に登録された個人認証情報（および各個人毎の装置に対する設定条件データ）とから、個人認証処理を行い、その結果を制御部８１９へ出力する。

【０１３２】制御部８１９では、リモコンコードデコード部８１７から入力された装置選択信号の値が、装置選択信号の値がＶＴＲを示している場合には、リモコンコードデコード部８１７から入力された機能選択信号と、個人認証処理部８１８より供給された個人認証処理結果にしたがい、前記図２および図３で説明した如く、即ち、前記個人認証処理部８１８において個人認証がパスしない場合には、記録，再生等のＶＴＲ８１４に関する一切の操作が禁止され、個人認証をパスした場合には、前記図示しない記録媒体に登録された各個人毎の装置に対する設定条件データの内の、個人認証された者の装置に対する設定条件データの登録内容（認証された者が有する記録や再生等を行う権利）に基づいて、ＶＴＲ８１４に対する記録，再生等の制御が為される。

【０１３３】一方、制御部８１９は、リモコンコードデコード部８１７から入力された装置選択信号の値が、ＶＴＲを示していない場合には、リモコンコードデコード部８１７から入力される機能選択信号は無視され、ＶＴＲ８１４に関する記録，再生等の一切の制御が禁止される（為されない）。

【０１３４】次に、個人認証を行わない装置であるテレビ８１３では、受信部８０８にて、前記リモコン８０１からの送信信号を受信する。受信部８０８で受信された信号は、例えば図１６（ｃ）に示す如くのデータフォーマットから成るリモコンコードに変換され、リモコンコードデコード部８１５に出力される。リモコンコードデコード部８１５では、受信部８０８より入力されたリモコンコード信号をデコードし、装置選択信号および機能選択信号を制御部８１６に出力する。

【０１３５】制御部８１６では、リモコンコードデコード部８１５から入力された装置選択信号の値が、テレビを示している場合には、リモコンコードデコード部８１５からの機能選択信号を受け付け、これに基づいてテレビジョン受像機の各種動作の制御が為される。

【０１３６】一方、リモコンコードデコード部８１５から入力された装置選択信号の値が、テレビを示していない場合には、リモコンコードデコード部８１５から入力された機能選択信号は無視され、これにより、テレビ８１３に関する一切の制御が禁止される（為されない）。

【０１３７】

【発明の効果】以上述べたように本発明によれば、記録再生装置に個人認証手段を装備し、装置を動作させる際、個人認証動作を行うようにしたので、装置が盗難にあった場合、正常に動作しないため盗難防止になる。また、個人使用（パーソナルユース）のための装置の場合、第三者による記録が出来ないため誤記録，誤消去を防ぐことができると共に、テープなどの媒体に記録されているパーソナル情報を保護することができる。さらに、認証手段の認証状況を、ＬＥＤ，ブザー，あるいはモニタ表示することにより、認証動作の進捗状況等を容易に確認することができる。

【０１３８】また、記録媒体自体に個人認証データを記録しておき、このデータをもとに個人認証を行い、カセットテープの管理を行うようにする構成としたので、誤って他人の重要な情報を消去してしまったり、或いは他人に消されることがなく、他人に見せたくないデータを保護することができ、盗難にあってもデータを再生される心配がない、などの効果が得られる。

【０１３９】そして、個人認証手段と記録再生装置の動

作スイッチとを兼ねた構成としたことにより、ユーザーは個人認証を行われていること意識することなく本発明の記録再生装置を使用することができる。

【０１４０】さらに、認証に際し（必要に応じ）、自動的に生体情報検出電極が現れるようにしたので、個人認証の必要が明示的に示されると共に、使用後、格納されるようにしたことにより、生体情報検出電極への異物等の付着を防止でき、生体情報検出電極の汚染を防ぐことができる。

【０１４１】また、再生テープから記録テープへとダビングする際、個人認証動作を行い、その結果に基づいてダビングの制限を設けるようにしたので、ソース側テープの著作権やプライバシーなどを、保護することができる。

【０１４２】さらに、暗号化またはスクランブルされた記録データを、ＤＶＣやＤＶＤ－ＲＡＭ等の記録媒体へ記録する際に、暗号化またはスクランブルを解くキーデータとして、登録されたユーザーの個人認証データそのまま、或いは認証データに所定の演算を施したものを用い、暗号化やスクランブルのためのキーデータを発生させ、このキーデータを用いて前記記録データを暗号化またはスクランブルし、記録するようにしたので、秘話性の非常に高い記録再生装置を実現することが可能となる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る生体情報による個人認証装置を具備した記録再生装置を示すブロック図である。

【図２】個人認証動作手順を示したフローチャートである。

【図３】メモリインカセットのメモリのデータストラクチャ例である。

【図４】本発明で個人認証を行うための生体情報検出手段として使用される指認証装置の一例を示すブロック図である。

【図５】指紋入力部を構成する表面形状センサの具体的な構成を示す図である。

【図６】指表面の抵抗値の測定原理を説明するための指紋入力部の等価画路である。

【図７】指認証装置の生体情報検出電極より得られる指紋情報を示す図である。

【図８】指がスイッチキーを押している状態を示した図である。

【図９】指がスイッチキーを引いている状態を示した図である。

【図１０】本発明に係る生体情報による個人認証装置を具備した記録再生装置の一例を示す図である。

【図１１】本発明に係る生体情報による個人認証装置を具備した記録再生装置の一例を示す図である。

【図１２】再生側装置および記録側装置の構成を示すブロック図である。

【図１３】ダビング動作を示したフローチャートである。

【図１４】本発明の実施の形態に係る生体情報検出電極を具備したリモコン装置を示すブロック図である。

【図１５】リモコンコード信号の生成手順の２つの例を示すフローチャートである。

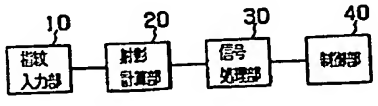
【図１６】本発明の実施の形態に係る生体情報検出電極を具備したマルチリモコン装置および被制御装置を示すブロック図である。

【図１７】従来の記録再生装置の構成を示すブロック図である。

【符号の説明】

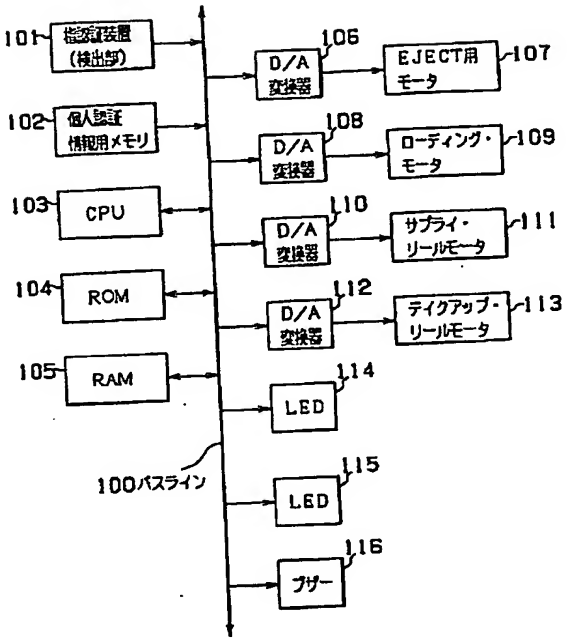
１０１…指認証装置（検出部）
１０２…個人認証情報用メモリ
１０３…ＣＰＵ
１０４…ＲＯＭ
１０５…ＲＡＭ
１０６…Ｄ／Ａ変換器
１０７…ＥＪＥＣＴ用モータ
１０８…Ｄ／Ａ変換器
１０９…ローディング・モータ
１１０…Ｄ／Ａ変換器
１１１…サプライ・リールモータ
１１２…Ｄ／Ａ変換器
１１３…テイクアップ・リールモータ
１１４…ＬＥＤ
１１５…ＬＥＤ
１１６…ブザー

【図４】

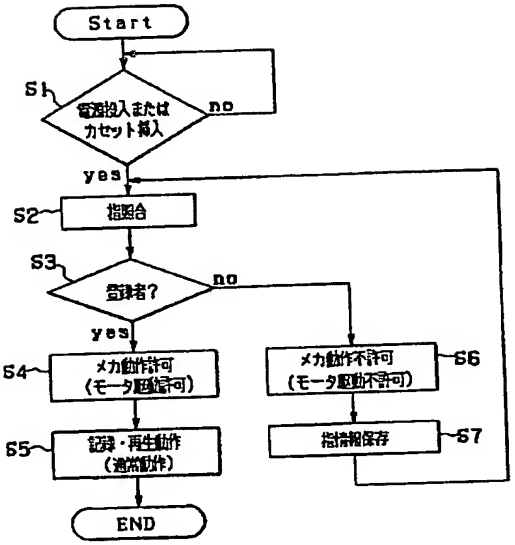


【図７】

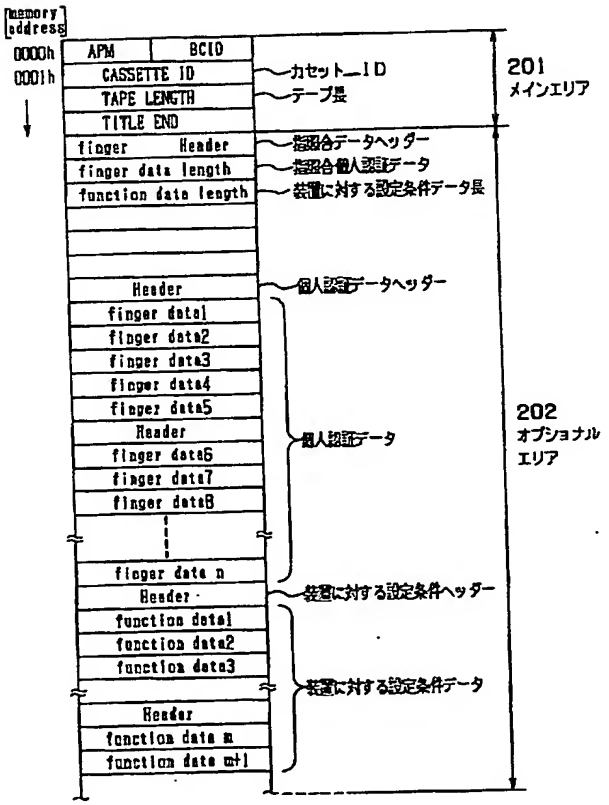
【図１】


101
指紋認識装置
(検出部)
102
個人認証
情報用メモリ
103
CPU
104
ROM
105
RAM
100バスライン
106
D/A
変換器
107
EJECT用
モータ
108
D/A
変換器
109
ローディング・
モータ
110
D/A
変換器
111
サプライ・
リールモータ
112
D/A
変換器
113
テイクアップ・
リールモータ
114
LED
115
LED
116
ブザー

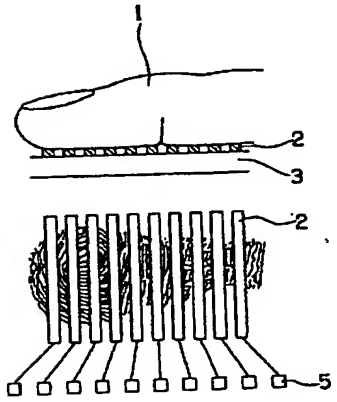
【図２】


Start
S1
電源投入または
カセット挿入
no
yes
S2
指照合
S3
登録者?
no
yes
S4
メカ動作許可
(モータ駆動許可)
S5
記録・再生動作
(通常動作)
S6
メカ動作不許可
(モータ駆動不許可)
S7
指情報保存
END

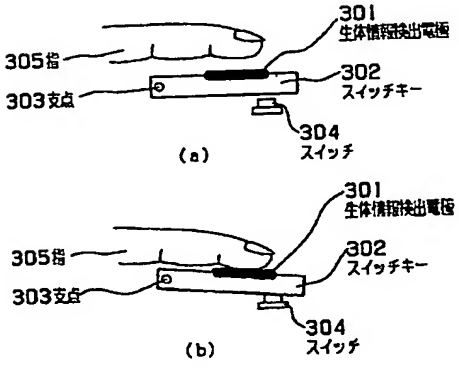
【図３】


memory address
0000h
0001h
APM
BCID
CASSETTE ID
TAPE LENGTH
TITLE END
finger Header
finger data length
function data length
Header
finger data1
finger data2
finger data3
finger data4
finger data5
Header
finger data6
finger data7
finger data8
finger data n
Header
function data1
function data2
function data3
Header
function data m
function data m+1
カセットID
テープ長
指照合データヘッダー
指照合個人認証データ
装置に対する設定条件データ長
個人認証データヘッダー
個人認証データ
装置に対する設定条件ヘッダー
装置に対する設定条件データ
201
メインエリア
202
オプショナル
エリア

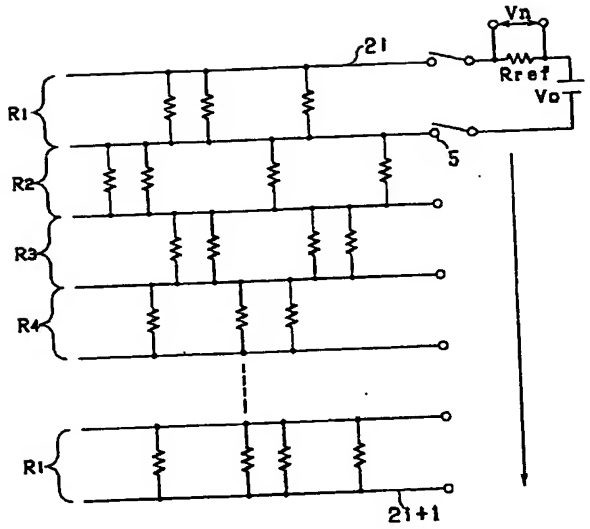
【図５】


1
2
3
2
5

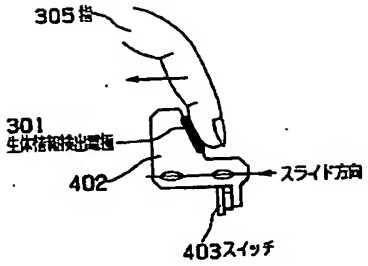
【図８】


301
生体情報検出電極
305指
302
スイッチキー
303支点
304
スイッチ
(a)
301
生体情報検出電極
305指
302
スイッチキー
303支点
304
スイッチ
(b)

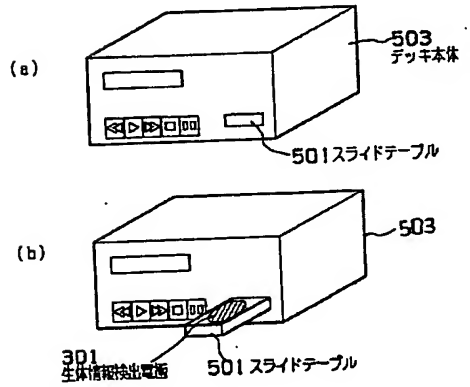
【図６】



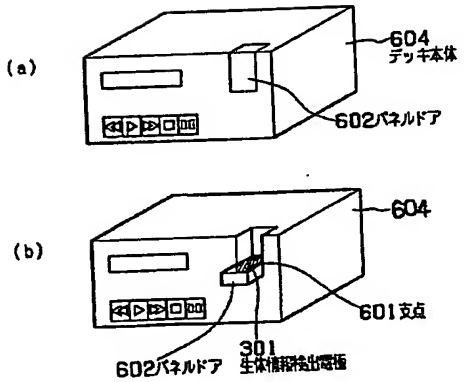
【図９】



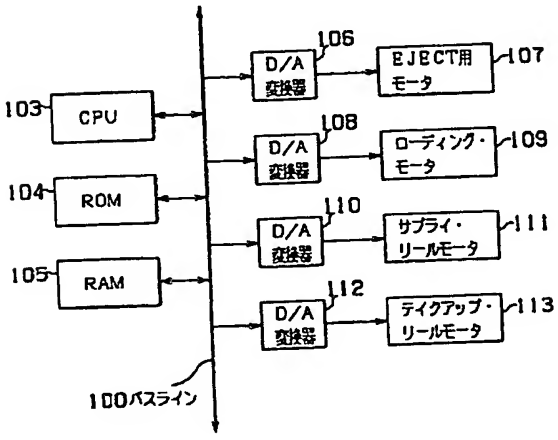
【図１０】



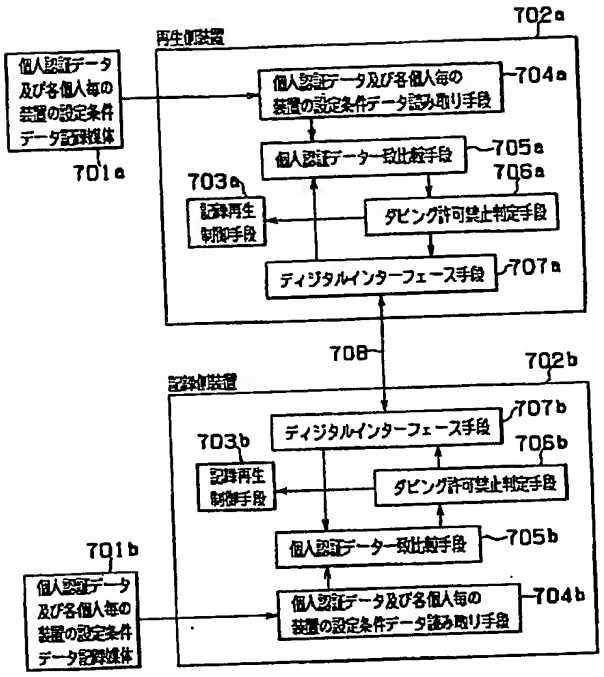
【図１１】



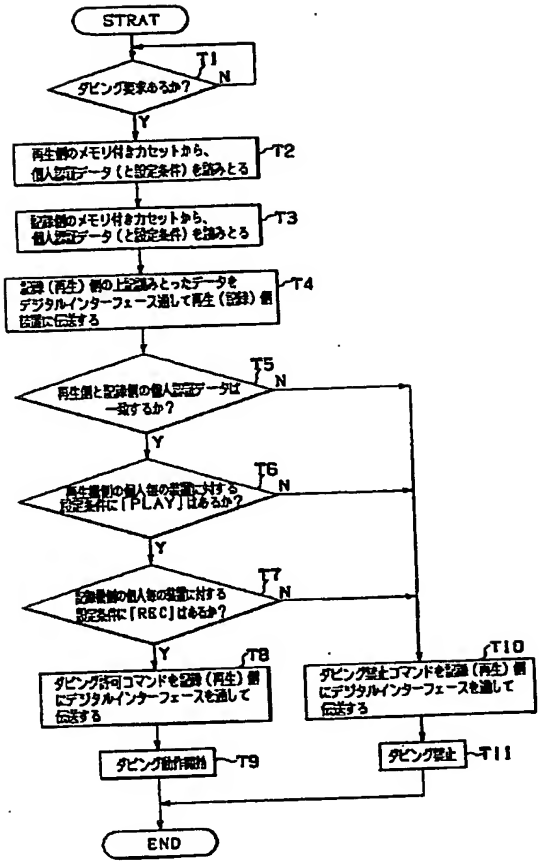
【図１７】



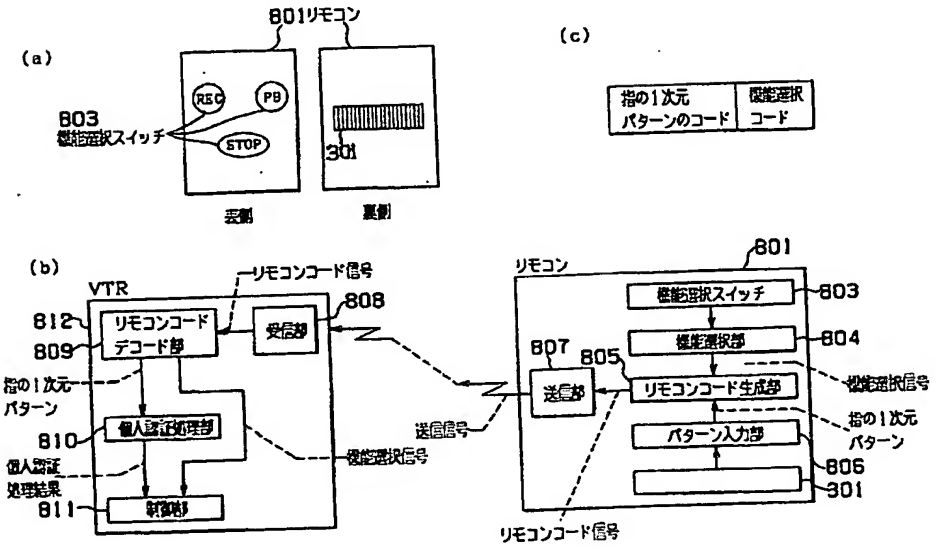
【図１２】


再生側装置
702a
個人認証データ及び各個人毎の装置の設定条件データ記録媒体
701a
個人認証データ及び各個人毎の装置の設定条件データ読み取り手段
704a
個人認証データ一致比較手段
705a
ダビング許可禁止判定手段
706a
記録再生制御手段
703a
ディジタルインターフェース手段
707a
708
記録側装置
702b
ディジタルインターフェース手段
707b
ダビング許可禁止判定手段
706b
記録再生制御手段
703b
個人認証データ一致比較手段
705b
個人認証データ及び各個人毎の装置の設定条件データ読み取り手段
704b
個人認証データ及び各個人毎の装置の設定条件データ記録媒体
701b

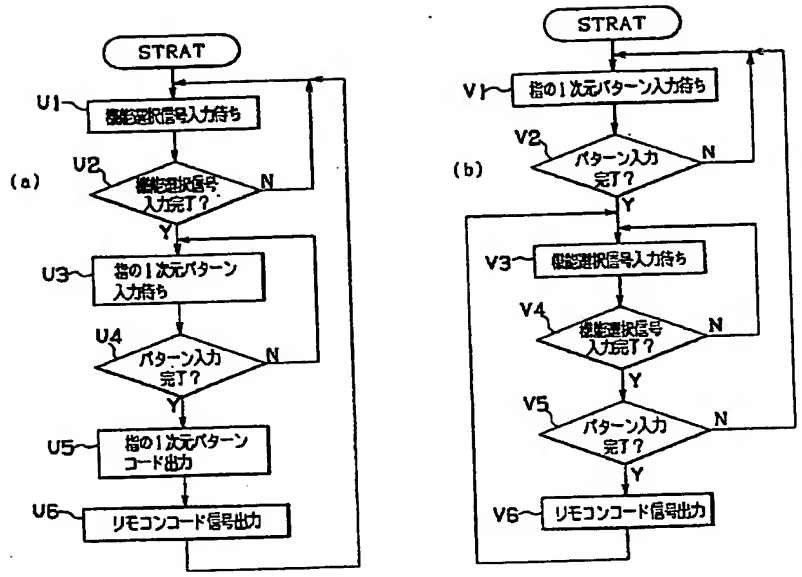
【図１３】


STRAT
T1
ダビング要求あるか?
N
Y
再生側のメモリ付き入力セットから、個人認証データ（と設定条件）を読みとる
T2
記録側のメモリ付き入力セットから、個人認証データ（と設定条件）を読みとる
T3
記録（再生）側の上記読みとったデータをデジタルインターフェース通して再生（記録）側装置に伝送する
T4
再生側と記録側の個人認証データは一致するか?
T5
N
Y
再生側の個人毎の装置に対する設定条件に「PLAY」はあるか?
T6
N
Y
記録側の個人毎の装置に対する設定条件に「REC」はあるか?
T7
N
Y
ダビング許可コマンドを記録（再生）側にデジタルインターフェースを通して伝送する
T8
ダビング禁止コマンドを記録（再生）側にデジタルインターフェースを通して伝送する
T10
ダビング動作開始
T9
ダビング禁止
T11
END

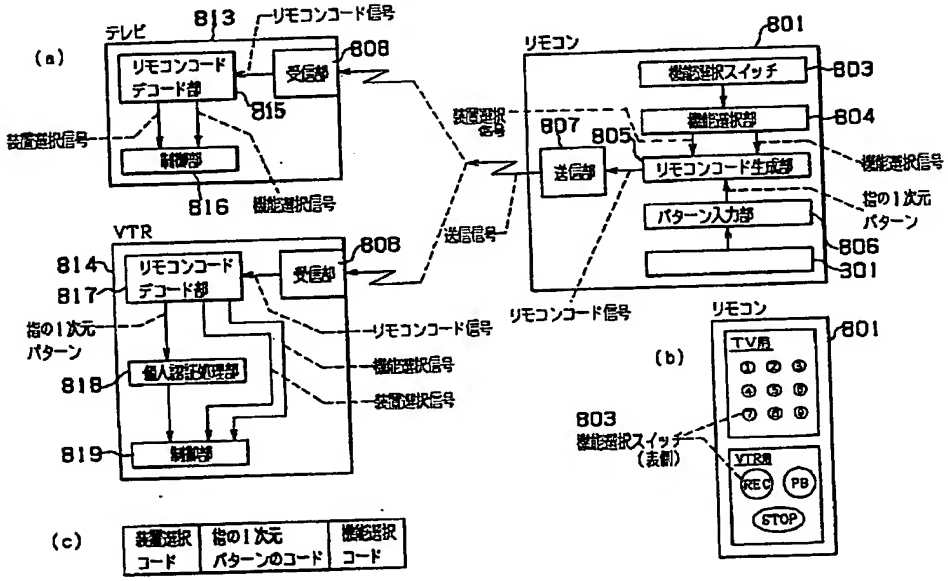
【図１４】


(a)
801リモコン
REC
PB
STOP
803
機能選択スイッチ
301
表側
裏側
(c)
指の1次元パターンのコード
機能選択コード
(b)
VTR
リモコンコード信号
812
リモコンコードデコード部
809
808
受信部
指の1次元パターン
810
個人認証処理部
個人認証処理結果
811
制御部
機能選択信号
送信信号
リモコン
801
機能選択スイッチ
803
機能選択部
804
807
805
送信部
リモコンコード生成部
機能選択信号
指の1次元パターン
パターン入力部
806
301
リモコンコード信号

【図１５】



【図１６】



フロントページの続き

(72)発明者　奥山　武彦
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝マルチメディア技術研究所内
(72)発明者　山田寺　真司
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝マルチメディア技術研究所内
(72)発明者　福島　道弘
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝マルチメディア技術研究所内
(72)発明者　大沢　真一
東京都港区新橋３丁目３番９号　東芝エー・ブイ・イー株式会社内